CRIMINAL OFFENSES AGAINST SECURITY OF COMPUTER DATA IN THE REPUBLIC OF SRPSKA ACCORDING TO THE CRIMINAL LAW OF 2017

Miodrag N. Simović[342]
Dragan Jovašević[343]
Vladimir M. Simović[344]

DOI: https://doi.org/10.31410/eraz.2018.746

Abstract: *In 2003, new criminal legislation came into force in Bosnia and Herzegovina. It is established on the basis of international standards, legal traditions, domestic and foreign legal theories and court practices, but also according to the needs of criminal policy. Of the four criminal laws (Bosnia and Herzegovina, the Federation of BiH, the Brčko District of Bosnia and Herzegovina and the Republic of Srpska) with numerous novelties, in 2017, the Republic of Srpska passed a completely new Criminal Code. This Code, starting with international obligations, in the first place the Convention on Cybercrime (Budapest) (2003), establishes a system of criminal offenses against the security of computer data, with a system of criminal responsibility and sanctions for natural and legal parties as well as the perpetrators of these criminal offenses. The concept, elements, characteristics and forms of computer crimes in the new legislation of the Republic of Srpska are discussed in this paper.*

Key words: *computer, abuse, criminal offense, responsibility, punishment, Republic of Srpska*.

1. Introduction

Chapter XXXII of the Criminal Code of the Republic of Srpska[345] under title „Criminal offences against security of computer data“ stipulates several criminal offences of this kind called computer, information or high-tech criminal offences.

Object of protection of these crimes is security of computer (information) data and systems, that is of computer network (Jovašević, Ikanović, 2012: 185-194). Today, it is common that the concept of computer crime includes these criminal offences. Aside from that, these criminal offences may also be called hi-tech crimes. This concept understands commission of criminal offences which have computers, computer networks, computer data, computer systems, and their products in material or electronic form, as objects or means of commission of criminal offences. This is a crime which very quickly and easily changes its shapes and forms of expression, boundaries between the states, and the type of damaged person (Jovašević, Mitrović, Ikanović, 2018: 722-733).

[342] Judge of the Constitutional Court of Bosnia and Herzegovina, Full Professor of the Faculty of Law of Banja Luka, Corresponding Member of the Academy of Sciences and Art of Bosnia and Herzegovina, Foreign Member of the Russian Academy of Natural Sciences and Active Member of the European Academy of Sciences and Arts, Bosnia and Herzegovina
[343] Full Professor of the Faculty of Law, Niš, *Serbia*
[344] Prosecutor of the Prosecutor's Office of Bosnia and Herzegovina and Associate Professor at the Faculty of Security and Protection Independent University in Banja Luka and Faculty of Law University „Vitez“ Vitez, Bosnia and Herzegovina
[345] „Službeni glasnik Republike Srpske“ broj 64/2017.

2. Damaging computer data and programmes

This is the first computer crime stipulated under Article 407 of the Criminal Code. It consists of unauthorized deletion, alteration, damage, concealement or otherwise making unusable a computer data or programme (Petrović, Jovašević, 2005: 278-285).

Object of protection is security of computer data or computer programme, and object of attack is: a) computer data or b) computer programme.

Execution has multiple alternative determinations.

The perpetrator of the crime may be any person, and the guilt requires intent.

A fine or sentence of imprisonment from six months to one year is prescribed for this crime. The perpetrator shall be obligatory imposed a security measure of seizure of equipment and devices used for commission of the criminal offence.

The first aggravated form of this crime, for which a sentence of six months to three years of imprisonment is prescribed, exists if the action taken in the execution of the crime caused damage amounting to over KM 10,000. The second aggravated form of this crime, for which a sentence of one to five years of imprisonment is prescribed, exists if the action taken in the execution of the crime caused material damage to another natural or legal person, amounting over KM 50,000 which amount is established according to market conditions are a time of commission of the criminal offence in question.

3. Computer sabotage

This crime is stipulated under Article 408 of the Criminal Code. It is committed by whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer data or programme or damages or destroys a computer or other device for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data important for republic authorities, public services, institutions, economic enterprises or other entities (Petrović, Jovašević, Ferhatović, 2016: 428-438).

The action of execution is alternatively determined (Turković *et al*., 2013: 341-347).

Capacity of damaged person constitutes an element of criminal offence (Đorđević, 2011: 177-182). It is required that a perpetrator, at a time of taking the action, has certain intention – to prevent (completely and permanently) or considerably disrupt (makes it more difficult) the procedure of electronic processing and transfer of data. It is not significant whether this intention in the specific case has been achieved, but that it exists at a time the perpetrator is taking the action of execution.

A sentence of imprisonment for a term of six months to five years is prescribed for this offence.

4. Generating and introducing computer viruses

This crime is stipulated under Article 409 of the Criminal Code and consists of generating a computer viruse with intention of its introduction into somebody else's computer, computer or telecommunication network (Babić, Marković, 2007: 206-207).

This crime is executed when generating – making previously non-existing computer virus which is capable, sufficient or which may cause certain changes or damages in use and usability of computers, computer or telecommunication network in its entirety or part of it (Pavišić, Grozdanić, Veić, 2007: 554-562). It is importatnt that the execution of this crime is taken with intention (as subjective element) – intention to introduce such generated computer virus into somebody else's computer, computer or telecommunication network. The perpetrator has to have the intention at a time the action was taken, notwithstanding whether the intention has been achieved in the specific case.

Perpetrator of the crime may be any person. As to the guilt a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment for a term of up to six months is prescribed. In addition to the sentence, the perpetrator is obligatory imposed a security measure of seizure of equipment or device used to commit the crime.

More aggravated form of this crime, for which a fine or sentence of imprisonment for a term of two years is prescribed, exists if a computer virus is introduced, indirectly or directly, into somebody else's computer or computer network, which, thereby causes damage (material or non-material). Accordingly, the consequence of a criminal offence appears in form of violation – damage caused to another natural or legal person, and even the whole state.

5. Computer fraud

This crime is stipulated under Article 410 of the Criminal Code. It consists of entering incorrect data, failure to enter correct data or otherwise concealing or falsely representing data, thereby affecting the results of electronic processing and transfer of data with intent to acquire for himself or another person unlawful material gain and thus causing material damage to another person (Mrvić Petrović, 2005: 321-325).

Object of protection is security of computer systems from entering incorrect and false data and trust in those systems (Đorđević, Đorđević, 2016: 191-194).

Perpetrator of the crime may be any person, and as to the guilt a direct intent characterized by mentioned intention is necessary. A fine or sentence of imprisonment for a term of up to three years is prescribed for this crime.

Less aggravated form of crime, for which a fine or sentence of imprisonment for a term of up to six months is prescribed, exists when a perpetrator committed a crime – concealing or false presentation of data in the computer or computer network in a legally prescribed manner with intention to cause damage to another person, that is to cause damage to another natural or legal person (Lazarević, Vučković, Vučković, 2004: 816-824). Malicious intention of the perpetrator to cause material or non-material damage to another person is a privileged circumstance.

The first more aggravated form, for which a sentence of imprisonment for a term of one to eight years is prescribed, exists when material gain (for perpetrator or another person) is acquired by action taken to commit a crime in the amount of over BAM 10,000. The amount of acquired material gain is a qualifying circumstance. It has to be in cause-and-effect connection with action taken to commit a crime.

The second form of more aggravated crime, for which a sentence of imprisonment for a term of two to ten years is prescribed, exists if a perpetrator acquired illegal material gain by action taken to commit a crime in the amount over BAM 30,000.

6. Unauthorized access to protected computers, computer networks, telecommunication network and electronic data processing

The criminal offence set out in Article 411 of the Criminal Code consists of access to a computer or computer network without authorization, or access to electronic data processing without authorization by breaching of protection measures, or in making, obtaining, sale or giving for use the instructions or means intended to enter into a computer system (Selinšek, 2007: 424-427).

Object of protection is security of a computer or computer network, or system of electronic data processing protected by a special technical and other protection measures (Simić, Trešnjev, 2010: 210-214).

Perpetrator of the crime may be any person having specific knowledge in the field of protection of computers or computer systems. As to the guilt a direct intent is necessary.

A fine or a sentence of imprisonment for a term of up to six months is prescribed for this crime.

The first more aggravated form of this crime, for which a fine or a sentence of imprisonment for a term of up to two years is prescribed, exists in case of recording or use of a computer data, obtained by accessing somebody else's computer or computer network, or somebody else's system of electronic data processing without authorization, given that it was done by breaching of protection measures. The second more aggravated form of this crime, for which a sentence of imprisonment for a term of up to three years is prescribed, exists if a accessing to somebody else's computer or computer network, or somebody else's system of electronic data processing without authorization by breaching protection measures: a) result in breach – suspension (disabling) or considerately disruption (making more difficult) the functioning of electronic processing and transfer of data or network, and b) results in other serious consequences. These consequences are a result of negligence of a perpetrator and are in cause-and-effect connection with taken action to commit a crime.

7. Preventing or restricting access to public computer network

This crime is stipulated under Article 412 of the Criminal Code. Object of protection is public computer network and free access to it by individually undefined number of persons. Motive of this incrimination is prevention of monopoly for using of public computer network (Petrović, Jovašević, Ferhatović, 2016: 428-437).

It is important that this action, in any of mentioned forms, is taken without authorization (by unauthorized person, without complying with requirements and assumptions and out of the proceedings prescribed under the law or other provisions regulating this field) in relation to public computer network (Jovašević, Ikanović, 2012: 185-197).

Perpetrator of the crime may be any person, and as to the guilt, a direct intent is necessary.

A fine or sentence of imprisonment for a term of up to one year is prescribed for this crime.

More aggravated form of this crime, for which a sentence of imprisonment for a term of up to three years is prescribed, exists if the crime is committed by: a) a particular person - an official, and b) in a specific manner - in discharge of his or her duty. Capacity of a perpetrator and manner of its commission constitute qualifying circumstances.

8. Unauthorized use of computer or computer network

This crime is stipulated under Article 413 of the Criminal Code. The crime consists of use of a computer services or computer networks without authorization and with intent to acquire unlawful material gain for himself or another person (Jovašević, Mitrović, Ikanović, 2017: 357-367).

Object of protection is legality and conscientiousness in use of computer system – services or network from all forms of abuse and negligence.

A perpetrator of crime may be any person, and as to the guilt a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment for a term of up to six months is prescribed for this crime. Prosecution for this crime is conducted upon a proposal.

9. Conclusion

The Criminal Code recognizes several criminal offences, established on the basis of obligations Bosnia and Herzegovina undertook by signing and ratifying of Budapest Convention on Computer Crime. These are criminal offences against safety of computer data, and the title itself of Head XXXII of the Code points out to the object of protection of these criminal offences. As objects of attack various legal goods appear, as well as the commission consists of various actions. Any person may appear as a perpetrator of these crimes, but in the practice these are persons having specific, special knowledge in computers or field of information technologies. These criminal offences, as a rule, are committed with intent, and in some cases, they are expressed as direct intent – due to existence of a certain intention (greedy or malicious) of the perpetrator at a time the crime was committed.

LITERATURE

Babić, M., Marković, I. (2007) *Krivično pravo, Posebni dio*, Banja Luka, str.206-207.
Đorđević, Đ. (2011) *Krivično pravo, Posebni deo*, Beograd, str. 177-182.
Đorđević, M., Đorđević, Đ. (2016) *Krivično pravo*, Beograd, str.191-194.
Jovašević, D. (2003) *Krivični zakon Republike Srbije sa sudskom praksom*, Beograd, str.351-361.
Jovašević, D. (2011) *Leksikon krivičnog prava*, Beograd, str. 419-421.
Jovašević, D. (2017) *Krivično pravo, Posebni deo*, Beograd, str.211-216.
Jovašević, D., Ikanović, V. (2012) *Krivično pravo Republike Srpske, Posebni deo*, Banja Luka, str. 185-194.
Jovašević, D., Mitrović, LJ., Ikanović, V. (2017) *Krivično pravo Republike Srpske, Posebni dio*, Banja Luka, str. 357-367.
Jovašević, D., Mitrović, LJ., Ikanović, V. (2018) *Komentar Krivičnog zakonika Republike Srpske*, Banja Luka, str. 722-733.
Kokolj, M., Jovašević, D. (2011) *Krivično pravo Republike Srpske, Opšti i posebni deo*,

Bijeljina, 357-369.
Lazarević, LJ., Vučković, B., Vučković, V. (2004) *Komentar Krivičnog zakonika Crne Gore*, Cetinje, str. 816-824.
Mrvić Petrović, N. (2005) *Krivično pravo*, Beograd, str. 321-325.
Pavišić, B., Grozdanić, V., Veić, P. (2007) *Komentar Kaznenog zakona*, Zagreb, str. 554-562.
Petrović, B., Jovašević, D. (2005) *Krivično pravo 2, Posebni dio.* Sarajevo, str. 278-285.
Petrović, B., Jovašević, D., Ferhatović, A. (2016) *Krivično pravo 2*, Sarajevo, str. 428-438.
Selinšek, LJ. (2007) *Kazensko pravo, Splošni del in osnove psoebnega dela*, Ljubljana, str. 424-427.
Simić, I., Trešnjev, A. (2010) *Krivični zakonik sa kraćim komentarom*, Beograd, str. 210-214.
Turković, K. *et al.* (2013) *Komentar Kaznenog zakona*, Zagreb, str. 341-347.